PCT/DE 99/03262

BUNDESREPUBLIK DEUTSCHLAND

REC'D 23 DEC 1999
WIPO PCT

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH
RULE 17.1(a) OR (b)

DE99/3262

Bescheinigung

EFU

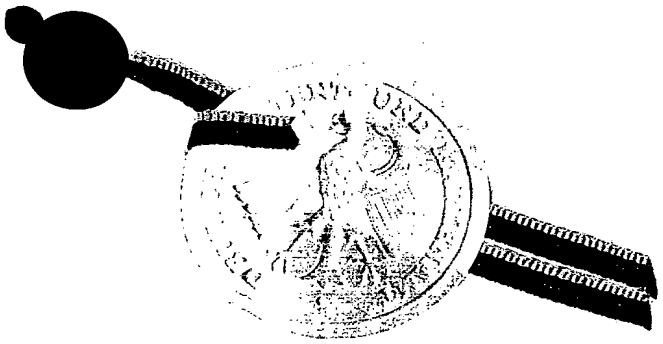
Die Siemens Aktiengesellschaft in München/Deutschland hat eine Patentanmeldung unter der Bezeichnung

"Verfahren und Anordnung zur Authentifikation von einer ersten Instanz und einer zweiten Instanz"

am 3. November 1998 beim Deutschen Patent- und Markenamt eingereicht.

Die angehefteten Stücke sind eine richtige und genaue Wiedergabe der ursprünglichen Unterlagen dieser Patentanmeldung.

Die Anmeldung hat im Deutschen Patent- und Markenamt vorläufig das Symbol H 04 L 9/30 der Internationalen Patentklassifikation erhalten.



München, den 16. November 1999
Deutsches Patent- und Markenamt
Der Präsident
Im Auftrag

Weihmayr

Aktenzeichen: 198 50 665.1

A 9161
06.90
11/98

198 50 665.1 vom 03.11.98

Beschreibung

Verfahren und Anordnung zur Authentifikation von einer ersten Instanz und einer zweiten Instanz

Die Erfindung betrifft ein Verfahren und eine Anordnung zur Authentifikation einer ersten Instanz mit einer zweiten Instanz und/oder umgekehrt.

Im Rahmen einer Authentifikation (auch: Authentifizierung) erklärt eine erste Instanz gegenüber einer zweiten Instanz verläßlich, daß sie auch tatsächlich die erste Instanz ist. Entsprechend ist bei der Übermittlung von (vertraulichen) Daten sicherzustellen, von wem diese tatsächlich stammen.

Ein symmetrisches Verschlüsselungsverfahren ist aus [1] bekannt. Bei dem symmetrischen Verschlüsselungsverfahren wird ein Schlüssel sowohl für die Ver- als auch für die Entschlüsselung verwendet. Ein Angreifer, der in den Besitz solch eines Schlüssels kommt, kann einen Klartext (die zu verschlüsselnde Information) in Schlüsseltext und umgekehrt transformieren. Das symmetrische Verschlüsselungsverfahren heißt auch Private-Key-Verfahren oder Verfahren mit geheimem Schlüssel. Ein bekannter Algorithmus zur symmetrischen Verschlüsselung ist der DES-Algorithmus (Data Encryption Standard). Er wurde im Jahre 1974 standardisiert unter ANSI X3.92-1981.

Ein asymmetrisches Verschlüsselungsverfahren ist aus [2] bekannt. Dabei ist einem Teilnehmer nicht ein einzelner, sondern ein Schlüsselsystem aus zwei Schlüsseln zugeordnet: Mit dem einen Schlüssel wird die Abbildung des Klartext in eine transformierte Form bewirkt, der andere Schlüssel ermöglicht die inverse Operation und überführt den transformierten Text in Klartext. Solch ein Verfahren heißt asymmetrisch, weil beide Seiten, die an einer kryptographischen Operation beteiligt sind, verschiedene

Schlüssel (eines Schlüsselsystems) einsetzen. Einer der beiden Schlüssel, z.B. ein Schlüssel p, kann öffentlich bekannt gemacht werden, wenn folgende Eigenschaften erfüllt sind:

- Es ist nicht mit vertretbarem Aufwand möglich, aus dem Schlüssel p einen zur inversen Operation notwendigen geheimen Schlüssel s abzuleiten.
- Selbst wenn Klartext mit dem (öffentlichen) Schlüssel p transformiert wird, ist es nicht möglich, daraus den (geheimen) Schlüssel s abzuleiten.

Aus diesem Grund heißt das asymmetrische Verschlüsselungsverfahren auch mit einem öffentlich bekanntmachbaren Schlüssel p Public-Key-Verfahren.

Grundsätzlich ist es möglich, den geheimen Schlüssel s aus dem öffentlichen Schlüssel p herzuleiten. Dies wird jedoch insbesondere dadurch beliebig aufwendig, daß Algorithmen gewählt werden, die auf Problemen der Komplexitätstheorie beruhen. Man spricht bei diesem Algorithmen auch von sogenannten "one-way-trapdoor"-Funktionen. Ein bekannter Vertreter für ein asymmetrisches Verschlüsselungsverfahren ist das Diffie-Hellman-Verfahren [6]. Dieses Verfahren läßt sich insbesondere zur Schlüsselverteilung (Diffie-Hellman key agreement, exponential key exchange) einsetzen.

Unter dem Begriff Verschlüsselung wird die allgemeine Anwendung eines kryptographischen Verfahrens V(x,k) verstanden, bei dem ein vorgegebener Eingabewert x (auch Klartext genannt) mittels eines Geheimnisses k (Schlüssel) in einen Chiffretext c := V(x,k) überführt wird. Mittels eines inversen Entschlüsselungsverfahrens kann durch Kenntnis von c und k der Klartext x rekonstruiert werden. Unter dem Begriff Verschlüsselung versteht man auch eine sogenannte Einweg-Verschlüsselung mit der Eigenschaft, daß es kein inverses, effizient berechenbares Entschlüsselungsverfahren gibt. Beispiele für solch ein Einweg-Verschlüsselungsverfahren ist

eine kryptographische Einwegfunktion bzw. eine kryptographische Hashfunktionen, beispielsweise der Algorithmus SHA-1, siehe [4].

Nun besteht in der Praxis das Problem, daß sichergestellt sein muß, daß ein öffentlicher Schlüssel, der zur Verifikation einer elektronischen Unterschrift eingesetzt wird, tatsächlich der öffentliche Schlüssel dessen ist, von dem man annimmt, daß er der Urheber der übermittelten Daten ist (Gewährleistung der Authentizität des Urhebers). Somit muß der öffentliche Schlüssel zwar nicht geheimgehalten werden, aber er muß authentisch sein. Es gibt bekannte Mechanismen (siehe [3]), die mit viel Aufwand sicherstellen, daß die Authentizität gewährleistet ist. Ein solcher Mechanismus ist die Einrichtung eines sogenannten Trustcenters, das Vertrauenswürdigkeit genießt und mit dessen Hilfe eine allgemeine Authentizität sichergestellt wird. Die Errichtung eines solchen Trustcenters und die Verteilung der Schlüssel von diesem Trustcenter aus sind jedoch überaus aufwendig. Beispielsweise muß bei der Schlüsselvergabe sichergestellt sein, daß auch wirklich der Adressat und kein potentieller Angreifer den Schlüssel bzw. die Schlüssel erhält. Dementsprechend hoch sich die Kosten für Einrichtung und Betrieb des Trustcenters.

Die **Aufgabe** der Erfindung besteht darin, eine Authentifikation sicherzustellen, wobei kein gesonderter Aufwand für eine Zertifizierungsinstanz oder ein Trustcenter investiert werden muß.

Diese Aufgabe wird gemäß den Merkmalen der unabhängigen Patentansprüche gelöst. Weiterbildungen der Erfindung ergeben sich auch aus den abhängigen Ansprüchen.

Zur Lösung der Aufgabe wird ein Verfahren zur Authentifikation von einer ersten Instanz mit einer zweiten Instanz angegeben, bei dem von der ersten Instanz eine

Operation A(x,g) auf einem (öffentlich) vorgegebenen bekannten Wert g und einem nur der ersten Instanz bekannten Wert x durchgeführt wird. Das Ergebnis der ersten Operation wird mit einem der ersten und der zweiten Instanz bekannten ersten Schlüssel verschlüsselt. Das mittels des ersten Schlüssels verschlüsselte Ergebnis der ersten Operation wird von der ersten Instanz zu der zweiten Instanz übermittelt.

Hierbei ist es besonders vorteilhaft, daß ein symmetrisches Verfahren eingesetzt wird, um eine Authentizität einer Instanz gegenüber einer weiteren Instanz herzustellen. Diese Authentizität wird bewirkt ohne Einrichtung einer gesonderten Zertifizierungsinstanz oder eines Trustcenters.

Eine Ausgestaltung besteht darin, daß die erste Operation A(x,g) ein asymmetrisches Kryptoverfahren ist. Insbesondere kann die erste Operation auf einer beliebigen endlichen und zyklischen Gruppe G durchgeführt werden.

Eine weitere Ausgestaltung besteht darin, daß die erste Operation A(x,g) eine Diffie-Hellman-Funktion $G(g^x)$ ist. Alternativ kann die erste Operation auch eine RSA-Funktion x^g sein.

Eine Weiterbildung besteht darin, daß die Gruppe G eine der folgenden Gruppen ist:

a) eine multiplikative Gruppe F_q^* eines endlichen Körpers F_q, insbesondere mit
   - einer multiplikativen Gruppe Z_p^* der ganzen Zahlen modulo einer vorgegebenen Primzahl p;
   - einer multiplikativen Gruppe F_t^* mit $t = 2^m$ über einem endlichen Körper F_t der Charakteristik 2;
   - einer Gruppe der Einheiten Z_n^* mit n als einer zusammengesetzten ganzen Zahl;

b) eine Gruppe von Punkten auf einer elliptischen Kurve über einem endlichen Körper;

c) eine Jacobivariante einer hyperelliptischen Kurve über einem endlichen Körper.

Eine andere Weiterbildung besteht darin, daß das Ergebnis der ersten Operation ein zweiter Schlüssel ist, mit dem die erste Instanz zur Wahrnehmung eines Dienstes auf der zweiten Instanz autorisiert wird.

Eine zusätzliche Ausgestaltung besteht darin, daß der zweite Schlüssel ein sogenannter "Sessionkey" oder eine an eine Applikation gebundene Berechtigung ist.

Auch ist es eine Weiterbildung, daß der zweite Schlüssel bestimmt wird zu

$$G(g^{xy})$$

indem von der zweiten Instanz eine Operation $G(g^{y})$ mit einer nur ihr bekannten geheimen Zahl y durchgeführt wird. Das Ergebnis dieser zweiten Operation wird mit dem ersten Schlüssel verschlüsselt und an die erste Instanz übermittelt.

Eine zusätzliche Weiterbildung besteht darin, daß zur Generierung des zweiten Schlüssels das Diffie-Hellmann-Verfahren eingesetzt wird.

Eine andere Ausgestaltung besteht darin, daß die Verschlüsselung mit dem ersten Schlüssel anhand einer Einwegfunktion, insbesondere einer kryptographischen Einwegfunktion durchgeführt wird. Eine Einwegfunktion zeichnet sich dadurch aus, daß sie in einer Richtung leicht zu berechnen, ihre Invertierung aber nur mit so großem Aufwand machbar ist, daß diese Möglichkeit in der Praxis vernachlässigt werden kann. Ein Beispiel für solch eine Einwegfunktion ist eine kryptographische Hashfunktion, die aus einer Eingabe A eine Ausgabe B erzeugt. Anhand der Ausgabe B kann nicht auf die Eingabe A rückgeschlossen

werden, selbst wenn der Algorithmus der Hashfunktion bekannt ist.

Auch ist es eine Weiterbildung, daß die Verschlüsselung, die mit dem ersten Schlüssel durchgeführt wird, einem symmetrischen Verschlüsselungsverfahren entspricht.

Schließlich ist es eine Weiterbildung, daß die übermittelten Daten vertrauliche Daten sind.

Weiterhin wird zur Lösung der Aufgabe eine Anordnung zur Authentifikation angegeben, bei der eine Prozessoreinheit vorgesehen ist, die derart eingerichtet ist, daß

a) von einer ersten Instanz eine erste Operation A(x,g) auf einem vorgegebenen bekannten Wert g und einem nur der ersten Instanz bekannten Wert x durchführbar ist;
b) bei dem das Ergebnis der ersten Operation mit einem der ersten und einer zweiten Instanz bekannten ersten Schlüssel verschlüsselbar ist;
c) bei dem das mit dem ersten Schlüssel verschlüsselte Ergebnis der ersten Operation von der ersten Instanz zu der zweiten Instanz übermittelbar ist;
d) bei dem von der zweiten Instanz mit dem ersten Schlüssel das Ergebnis der ersten Operation entschlüsselt wird und somit die erste Instanz authentifizierbar ist.

Diese Anordnung ist insbesondere geeignet zur Durchführung des erfindungsgemäßen Verfahrens oder einer seiner vorstehend erläuterten Weiterbildungen.

Ausführungsbeispiele der Erfindung werden nachfolgend anhand der Zeichnung dargestellt und erläutert.

Es zeigen

Fig.1 eine Skizze zur Vereinbarung eines gemeinsamen Schlüssels zwischen zwei Instanzen, deren jede Authentizität jeweils sichergestellt ist;

Fig.2 eine Skizze gemäß Fig.1 unter Einsatz des DES-Algorithmus;

Fig.3 eine Prozessoreinheit.

In **Fig.1** ist eine Skizze dargestellt zur Vereinbarung eines gemeinsamen Schlüssels zwischen zwei Instanzen, deren jede Authentizität jeweils sichergestellt ist. Eine Instanz A 101 wählt eine zufällige Zahl x in einem Körper "mod p-1" (siehe Block 103). Nun wird von der Instanz 101 an eine Instanz 102 eine Nachricht 104 geschickt, die folgendes Format aufweist:

$$g,\ p,\ T_A,\ ID_A,\ g^x \bmod p,\ H(g^x \bmod p,\ PW,\ ID_A,\ T_A,\ldots),$$

wobei

x	einen geheimen Zufallswert der Instanz A 101,
y	einen geheimen Zufallswert der Instanz B 102,
g	einen Generator nach dem Diffie-Hellman-Verfahren,
p	eine Primzahl für das Diffie-Hellman-Verfahren,
T_A	einen Zeitstempel der Instanz A beim Erzeugen bzw. Absenden der Nachricht,
T_B	einen Zeitstempel der Instanz B beim Erzeugen bzw. Absenden der Nachricht,
ID_A	ein Identifikationsmerkmal der Instanz A,
ID_B	ein Identifikationsmerkmal der Instanz B,
$g^x \bmod p$	ein öffentlicher Diffie-Hellman-Schlüssel der Instanz A,

$g^y \bmod p$	ein öffentlicher Diffie-Hellman-Schlüssel der Instanz B,
PW	ein gemeinsames Geheimnis zwischen den Instanzen A und B (Paßwort, "shared secret"),
H(M)	eine kryptographische Einwegfunktion (Hashfunktion) über die Parameter M,
KEY	ein beiden Instanzen A und B gemeinsamer Sessionkey.

bezeichnen. Ist diese Nachricht bei der Instanz 102 angekommen, wird dort (siehe Block 105) eine zufällige Zahl y aus dem Körper "mod p-1" gewählt und in einem Block 106 ein gemeinsamer Schlüssel vereinbart zu

$$KEY = g^{xy} \bmod p.$$

Die zweite Instanz 102 übermittelt eine Nachricht 107 mit dem Format

$$T_B,\ ID_B,\ g^y \bmod p,\ H(g^y \bmod p,\ PW,\ ID_B,\ T_B,...)$$

an die erste Instanz 101. Die erste Instanz 101 wird daraufhin in einem Schritt 108 die Operation

$$KEY = g^{xy} \bmod p$$

aus, woraus sich ebenfalls der gemeinsame Schlüssel KEY ergibt.

Hierbei sei ausdrücklich angemerkt, daß beispielhaft der Körper "mod p-1" als eine von vielen Möglichkeiten herausgegriffen wurde. Ferner werden die Nachrichten 104 und 107 als jeweils eine Möglichkeit von vielen angesehen. Insbesondere sind die zur Adressierung angeführten Felder innerhalb der Nachrichten abhängig von der Applikation bzw. dem verwendeten Übertragungsprotokoll.

In Fig.1 wird eine kryptographische Einweg-Hashfunktion H verwendet. Ein Beispiel zur Übermittlung einer solchen Einweg-Hashfunktion ist der SHA-1-Algorithmus (vergleiche [4]). Der Einsatz eines symmetrischen Verschlüsselungsverfahrens, z.B. des DES-Algorithmus [5], anstatt der Einweg-Hashfunktion H, wird in **Fig.2** dargestellt. Die Blöcke 101, 102, 103, 105, 106 und 108 sind in Fig.2 identisch zu Fig.1. Die von der ersten Instanz 101 an die zweite Instanz 102 übertragene Nachricht 201 hat das Format

$$g,\ p,\ T_A,\ ID_A,\ g^x \bmod p,\ ENC_{PW}(g^x \bmod p,\ PW,\ ID_A,\ T_A, \ldots),$$

wobei

$ENC_{PW}(M)$ ein symmetrisches Verfahren zur Verschlüsselung des Parameters M mit dem Schlüssel PW

bezeichnet.

In umgekehrter Richtung wird von der Instanz 102 an die Instanz 101 in Fig.2 die Nachricht 202 verschickt, die folgendes Format aufweist:

$$T_B,\ ID_B,\ g^y \bmod p,\ ENC_{PW}(g^y \bmod p,\ PW,\ ID_B,\ T_B, \ldots).$$

Hierbei sei insbesondere vermerkt, daß jeweils eine Nachricht (in Fig.1 die Nachricht 104 bzw. in Fig.2 die Nachricht 201) ausreicht, um die erste Instanz 101 gegenüber der zweiten Instanz 102 zu authentifizieren. Sieht man davon ab, daß sich auch die zweite Instanz 102, beispielsweise ein wahrzunehmender Dienst innerhalb einer Netzwerkverbindung, z.B. dem Internet, authentifizieren muß, so kann es ausreichen, wenn lediglich die erste Instanz 101 sich authentifiziert. Dies ist bereits nach Übertragung der jeweils ersten Nachrichten 104 und 201 gegeben. Wählt sich insbesondere die erste Instanz 101 bei der zweiten Instanz 102 ein, so ist häufig davon auszugehen, daß diese zweite

Instanz 102 auch die richtige Instanz ist. Umgekehrt muß die zweite Instanz 102 davon ausgehen können, daß der Anrufer (die erste Instanz 101) auch der ist, für den er sich ausgibt. Somit ist in dieser Richtung, von der ersten Instanz 101 zur zweiten Instanz 102, die Prüfung der Authentizität wichtig.

In **Fig.3** ist eine Prozessoreinheit PRZE dargestellt. Die Prozessoreinheit PRZE umfaßt einen Prozessor CPU, einen Speicher SPE und eine Input/Output-Schnittstelle IOS, die über ein Interface IFC auf unterschiedliche Art und Weise genutzt wird: Über eine Grafikschnittstelle wird eine Ausgabe auf einem Monitor MON sichtbar und/oder auf einem Drucker PRT ausgegeben. Eine Eingabe erfolgt über eine Maus MAS oder eine Tastatur TAST. Auch verfügt die Prozessoreinheit PRZE über einen Datenbus BUS, der die Verbindung von einem Speicher MEM, dem Prozessor CPU und der Input/Output-Schnittstelle IOS gewährleistet. Weiterhin sind an den Datenbus BUS zusätzliche Komponenten anschließbar, z.B. zusätzlicher Speicher, Datenspeicher (Festplatte) oder Scanner.

Literaturverzeichnis:

[1] Christoph Ruland: Informationssicherheit in Datennetzen, DATACOM-Verlang, Bergheim 1993, ISBN 3-89238-081-3, Seiten 42-46.

[2] Christoph Ruland: Informationssicherheit in Datennetzen, DATACOM-Verlang, Bergheim 1993, ISBN 3-89238-081-3, Seiten 73-85.

[3] Christoph Ruland: Informationssicherheit in Datennetzen, DATACOM-Verlang, Bergheim 1993, ISBN 3-89238-081-3, Seiten 101-117.

[4] NIST, FIPS PUB 180-1: Secure Hash Standard, April 1995; http://csrc.nist.gov/fips/fip180-1.ps

[5] NIST, FIPS PUB 81: DES Modes of Operation, December 1980; http://www.itl.nist.gov/div897/pubs/fip81.htm

[6] A. Menezes, P. v. Oorschot, S. Vanstone: Handbook of Applied Cryptography; CRC Press 1996, ISBN 0-8493-8523-7; chapter 12.6 (pp. 515-524).

Patentansprüche

1. Verfahren zur Authentifikation,

a) bei dem von einer ersten Instanz eine erste Operation A(x,g) auf einem vorgegebenen bekannten Wert g und einem nur der ersten Instanz bekannten Wert x durchgeführt wird;

b) bei dem das Ergebnis der ersten Operation mit einem der ersten und einer zweiten Instanz bekannten ersten Schlüssel verschlüsselt wird;

c) bei dem das mit dem ersten Schlüssel verschlüsselte Ergebnis der ersten Operation von der ersten Instanz zu der zweiten Instanz übermittelt wird;

d) bei dem von der zweiten Instanz mit dem ersten Schlüssel das Ergebnis der ersten Operation entschlüsselt wird und somit die erste Instanz authentifiziert wird.

2. Verfahren nach Anspruch 1,
bei dem die erste Operation A(x,g) ein asymmetrisches Kryptoverfahren ist.

3. Verfahren nach Anspruch 1 oder 2,
bei dem die erste Operation A(g,x)

a) eine Diffie-Hellman-Funktion $G(g^x)$ ist, wobei G() eine beliebige, endliche zyklische Gruppe G ist;

b) eine RSA-Funktion x^g ist.

4. Verfahren nach einem der vorhergehenden Ansprüche,
bei dem die erste Operation auf einer Gruppe G durchgeführt wird, wobei die Gruppe G eine der folgenden Gruppen ist:

a) eine multiplikative Gruppe F_q^* eines endlichen Körpers F_q, insbesondere mit

- einer multiplikativen Gruppe Z_p^* der ganzen Zahlen modulo einer vorgegebenen Primzahl p;

- einer multiplikativen Gruppe F_t^* mit $t = 2^m$ über einem endlichen Körper F_t der Charakteristik 2;
- einer Gruppe der Einheiten Z_n^* mit n als einer zusammengesetzten ganzen Zahl;

b) eine Gruppe von Punkten auf einer elliptischen Kurve über einem endlichen Körper;

c) eine Jacobivariante einer hyperelliptischen Kurve über einem endlichen Körper.

5. Verfahren nach einem der vorhergehenden Ansprüche, bei dem das Ergebnis der ersten Operation ein zweiter Schlüssel ist, mit dem die erste Instanz zur Wahrnehmung eines Dienstes auf der zweiten Instanz autorisiert wird.

6. Verfahren nach dem vorhergehenden Anspruch, bei dem der zweite Schlüssel ein Sessionkey oder eine an eine Applikation gebundene Berechtigung ist.

7. Verfahren nach einem der Ansprüche 5 oder 6, bei dem der zweite Schlüssel bestimmt wird zu

$$G(g^{xy}),$$

indem von der zweiten Instanz eine zweite Operation $G(g^y)$ mit einer nur ihr bekannten geheimen Zahl y durchgeführt, das Ergebnis dieser zweiten Operation mit dem ersten Schlüssel verschlüsselt und an die erste Instanz übermittelt wird.

8. Verfahren nach einem der vorhergehenden Ansprüche, bei dem zur Erzeugung des zweiten Schlüssels das Diffie-Hellman-Verfahren eingesetzt wird.

9. Verfahren nach einem der vorhergehenden Ansprüche, bei dem die Verschlüsselung mit dem ersten Schlüssel anhand einer Einwegfunktion, insbesondere einer kryptographischen Einwegfunktion, durchgeführt wird.

10. Verfahren nach einem der Ansprüche 1 bis 6, bei dem die Verschlüsselung mit dem ersten Schlüssel anhand eines symmetrischen Verschlüsselungsverfahrens durchgeführt wird.

11. Verfahren nach einem der vorhergehenden Ansprüche, bei dem die übermittelten Daten vertrauliche Daten sind.

12. Anordnung zur Authentifikation, bei der eine Prozessoreinheit vorgesehen ist, die derart eingerichtet ist, daß

a) von einer ersten Instanz eine erste Operation A(x,g) auf einem vorgegebenen bekannten Wert g und einem nur der ersten Instanz bekannten Wert x durchführbar ist;

b) bei dem das Ergebnis der ersten Operation mit einem der ersten und einer zweiten Instanz bekannten ersten Schlüssel verschlüsselbar ist;

c) bei dem das mit dem ersten Schlüssel verschlüsselte Ergebnis der ersten Operation von der ersten Instanz zu der zweiten Instanz übermittelbar ist;

d) bei dem von der zweiten Instanz mit dem ersten Schlüssel das Ergebnis der ersten Operation entschlüsselt wird und somit die erste Instanz authentifizierbar ist.

Zusammenfassung

Verfahren und Anordnung zur Authentifikation von einer ersten Instanz und einer zweiten Instanz

Um eine erste Instanz bei einer zweiten Instanz zu authentifizieren, wird mittels eines asymmetrischen Kryptoverfahrens eine erste Zahl erzeugt. Diese erste Zahl wird symmetrisch verschlüsselt und an die zweite Instanz übertragen. Die zweite Instanz überprüft die erste Zahl durch Entschlüsselung der zweiten Zahl und authentifiziert damit die erste Instanz.

FIG 1

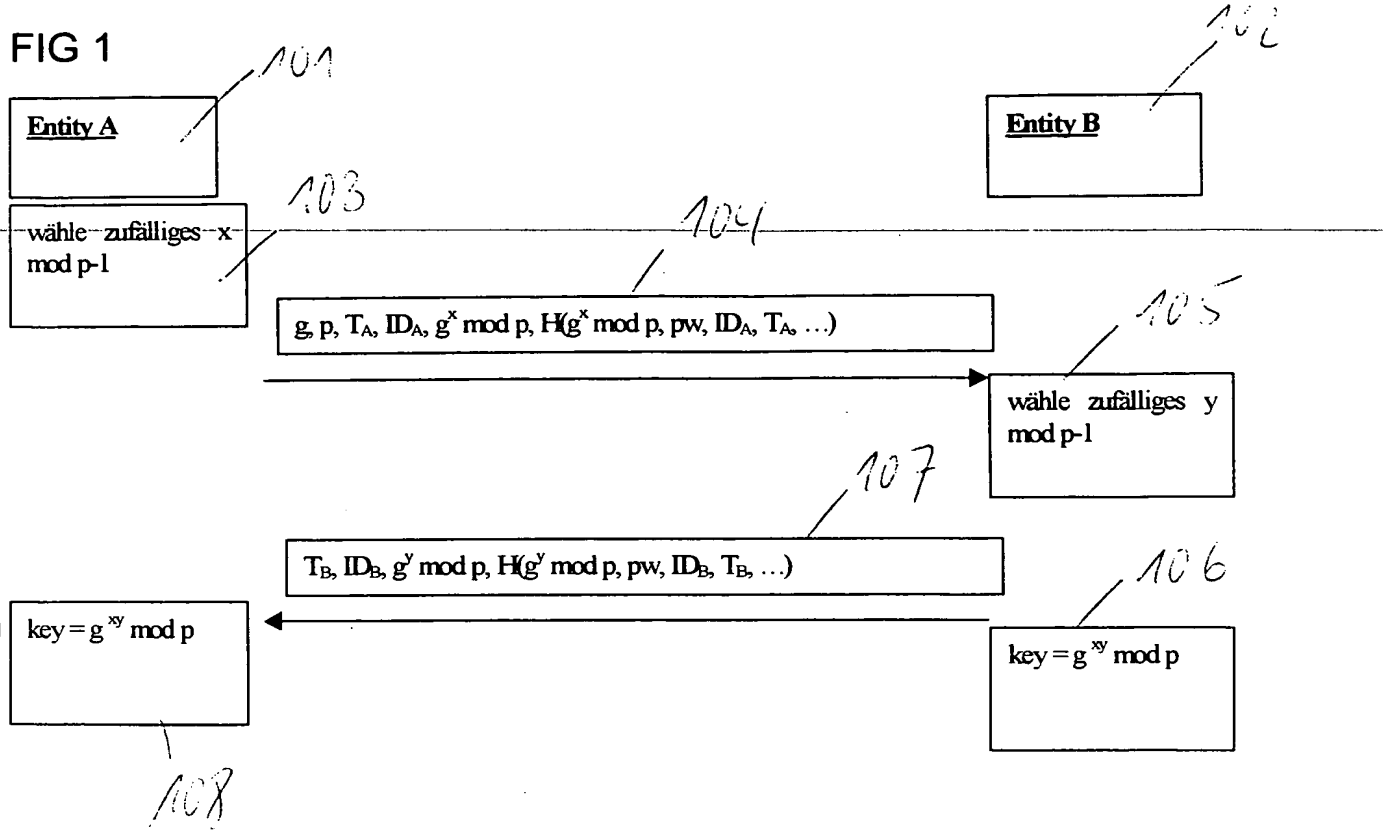

101
Entity A
102
Entity B
103
wähle zufälliges x mod p-1
104
g, p, T_A, ID_A, g^x mod p, H(g^x mod p, pw, ID_A, T_A, ...)
105
wähle zufälliges y mod p-1
107
T_B, ID_B, g^y mod p, H(g^y mod p, pw, ID_B, T_B, ...)
106
key = g^{xy} mod p
key = g^{xy} mod p
108

FIG 2

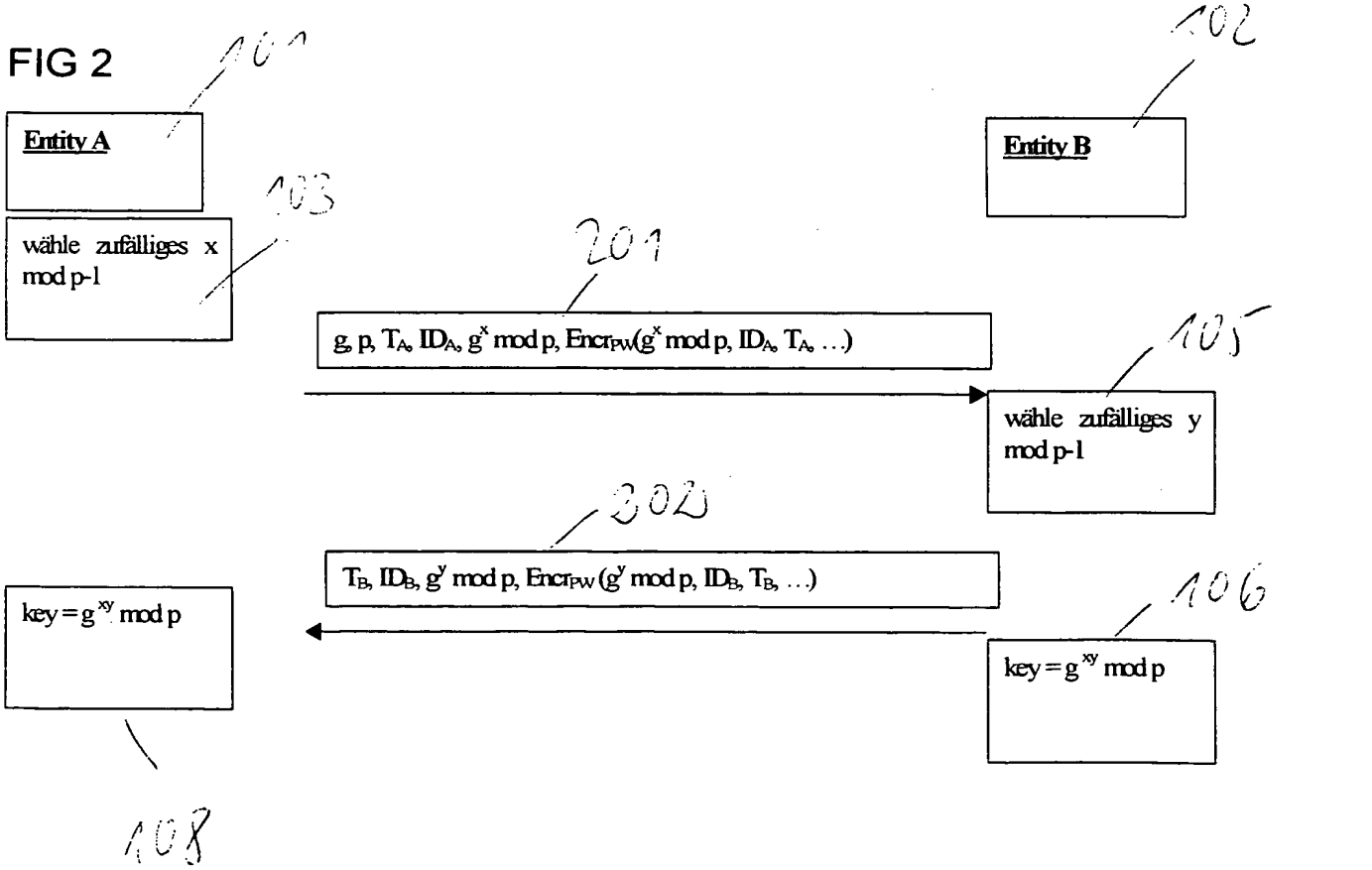
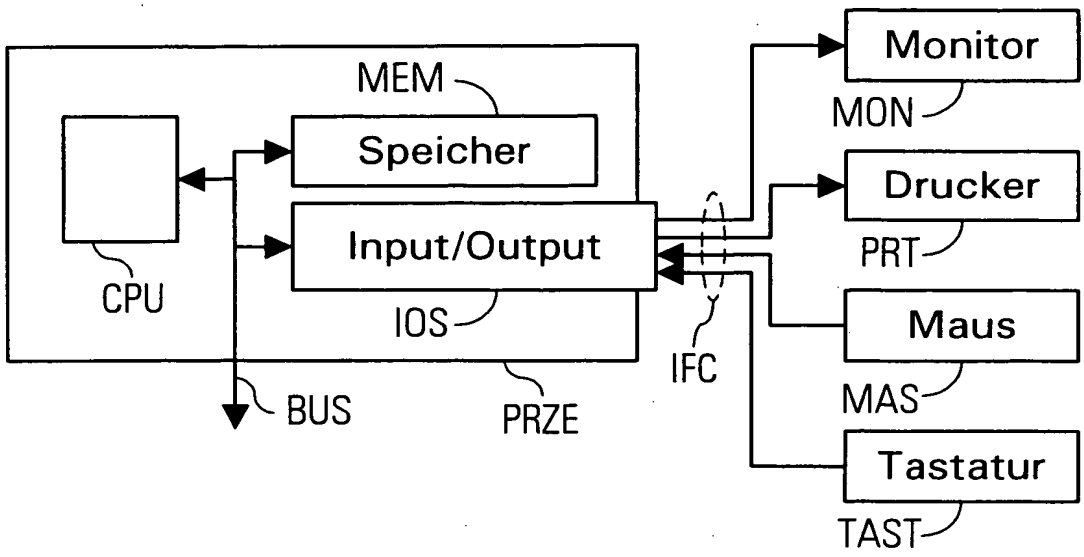

101
Entity A
102
Entity B
103
wähle zufälliges x mod p-1
201
g, p, T_A, ID_A, g^x mod p, $Encr_{PW}$(g^x mod p, ID_A, T_A, ...)
105
wähle zufälliges y mod p-1
202
T_B, ID_B, g^y mod p, $Encr_{PW}$(g^y mod p, ID_B, T_B, ...)
106
key = g^{xy} mod p
key = g^{xy} mod p
108

FIG 3


MEM
Speicher
Input/Output
IOS
CPU
BUS
PRZE
IFC
Monitor
MON
Drucker
PRT
Maus
MAS
Tastatur
TAST